



# Zscaler Internet Access

AI-powered protection for  
all users, all apps, all locations

Zscaler Internet Access™ defines safe, fast internet and SaaS access with the industry's first and only AI-powered security service edge (SSE) platform.

## Legacy network security has become ineffective in a cloud- and mobile-first world

Legacy hub-and-spoke architectures were effective when users were located primarily at headquarters or in a branch office, applications resided solely in the corporate data center, and your attack surface was limited to what your organization sanctioned. Today, we live in a drastically different world, with a threat landscape in which ransomware, encrypted threats, supply chain attacks, and other advanced threats break through legacy network defenses. It's time to find a cloud native security solution that holistically reduces risk and complexity while enabling flexibility to help drive business initiatives forward.

## Zscaler Internet Access

Securing today's cloud- and mobile-first enterprise requires a fundamentally different approach built on zero trust. Zscaler Internet Access, part of the Zscaler Zero Trust Exchange™, is the world's most deployed security service edge (SSE) platform, built on a decade of secure web gateway leadership.

### Benefits:

- **Prevent cyberthreats and data loss with AI:** Protect your organization against advanced threats with a suite of AI-powered cyberthreat and data protection services, enriched by real-time updates sourced from 300 trillion daily threat signals from the world's largest security cloud.
- **Get an unmatched user experience:** Get the world's fastest internet and SaaS experience (up to 40% faster than legacy security architectures) to boost productivity and increase business agility.
- **Modernize your security architecture:** Realize 139% ROI with Zscaler by replacing 90% of your costly, complex, and slow appliances with a fully cloud-native zero trust platform.

Delivered as a scalable SaaS platform from the world's largest security cloud, it eliminates legacy network security solutions to stop advanced attacks and prevent data loss with a comprehensive zero trust approach, offering:

**Best-in-class, consistent security for today's hybrid workforce:** When you move security to the cloud, all users, apps, devices, and locations get always-on threat protection based on identity and context. Your security policy goes everywhere your users go.

**Lightning-fast access with zero infrastructure:** Direct-to-cloud architecture ensures a fast, seamless user experience. This eliminates backhauling, improves performance and user experience, and simplifies network administration—with no physical infrastructure, ever.

**AI-powered protection from the world's largest security cloud:** Inline inspection of all internet and SaaS traffic, including SSL decryption, with a suite of AI-powered cloud security services to stop ransomware, phishing, zero-day malware, and advanced attacks based on threat intelligence from 300 trillion daily signals.

**Simplified management:** Using a cloud native security solution infused with AI, no hardware to manage, streamlined workflows, and business-focused policy creation frees up valuable time for your team to focus on strategic goals.

## Integrated, AI-powered security and data protection services

Zscaler Internet Access includes a comprehensive suite of AI-powered security and data protection services to help you stop cyberattacks and data loss. As a fully cloud-delivered SaaS solution, you can add new capabilities without any additional hardware or lengthy deployment cycles. The modules available as part of Zscaler Internet Access are:

- **Cloud Secure Web Gateway (SWG):** Deliver a safe, fast web experience that eliminates ransomware, malware, and other advanced attacks with real-time, AI-powered analysis and URL filtering from the only leader in the [2020 Gartner MQ for SWGs](#).
- **Cloud Access Security Broker (CASB):** Secure cloud apps with integrated CASB to protect data, stop threats, and ensure compliance across your SaaS and IaaS environments.
- **Cloud Data Loss Prevention (DLP):** Protect data in motion with full inline inspection and advanced measures like exact data match (EDM), optical character recognition (OCR), and machine learning.

**Zscaler named a Leader  
in the Gartner Magic  
Quadrant for SSE**

[Learn More →](#)

**Gartner**

- **Cloud Firewall & IPS:** Extend industry-leading protection to all ports and protocols, and replace edge and branch firewalls with a cloud native platform.
- **Cloud Sandbox:** Stop never-before-seen and elusive malware across web and file transfer protocols with AI-driven quarantine, sharing consistent and global protection across all users in real time.
- **AI-Powered Cloud Browser Isolation:** Make web-based attacks obsolete and prevent data loss by creating a virtual air gap between users, the web, and SaaS.
- **Digital Experience Monitoring:** Reduce IT operational overhead and speed up ticket resolution with a unified view of application, cloud path, and endpoint performance metrics for analysis and troubleshooting.

## Zscaler Internet Access for Users and Workloads

Eliminate risk for cloud workloads accessing any internet or SaaS destination with Zscaler Internet Access. By removing the need for workloads to access the internet through legacy, network-centric tools such as VPNs, firewalls (including virtual firewalls), or WAN technologies, you can prevent compromise and stop lateral movement without requiring a patchwork of security tools. By applying ZIA's comprehensive suite of security and data protection capabilities to workloads, you can unify zero trust security for your users and workloads with a single, integrated platform.

By pairing ZIA with **Zscaler Private Access**, you can extend protection to your private apps and workloads, whether they reside in the public cloud or a private data center.

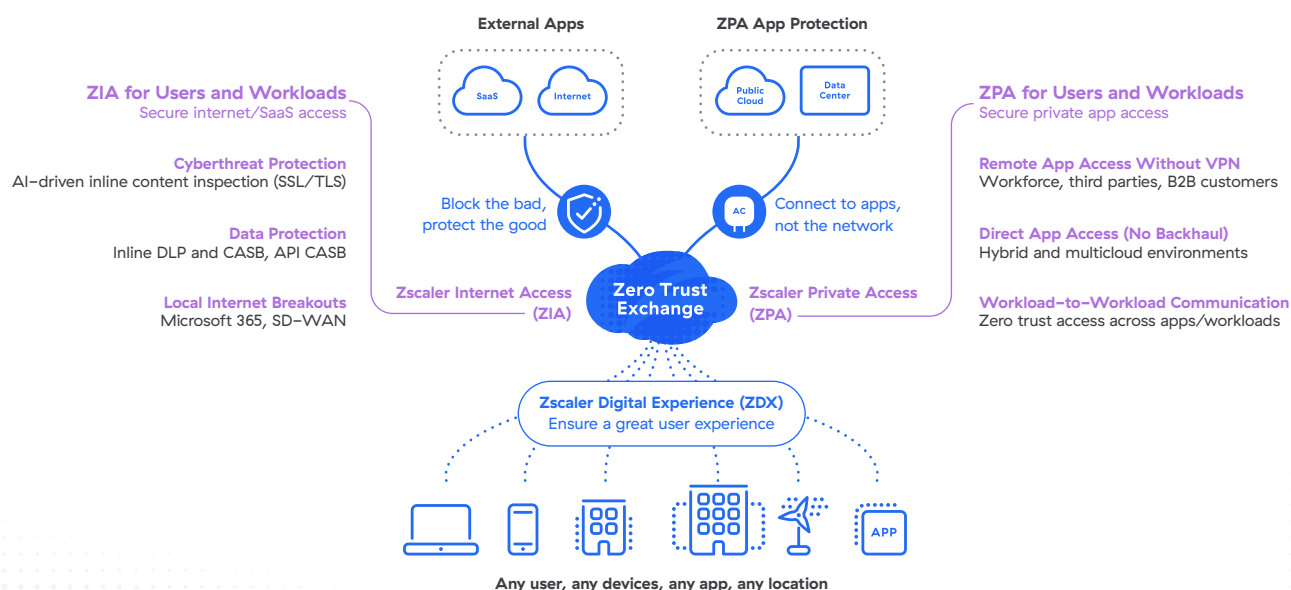


Figure 1: The Zero Trust Exchange

## Use cases



### Cyberthreat and ransomware protection

Move from legacy network security to Zscaler's revolutionary zero trust architecture that prevents compromise, eliminates the attack surface, stops lateral movement, and keeps data safe.

[Learn More →](#)



### Secure hybrid workforce

Empower employees, partners, customers, and suppliers to securely access web applications and cloud services from anywhere, on any device—and ensure a great digital experience.

[Learn More →](#)



### Data protection

Stop data loss from users, SaaS apps, and public cloud infrastructure from accidental exposure, data theft, or double-extortion ransomware.

[Learn More →](#)



### Infrastructure modernization

Eliminate costly, complex networks with fast, secure, direct-to-cloud access that removes the need for edge and branch firewalls.

[Learn More →](#)

## The Zscaler Zero Trust Exchange Ecosystem

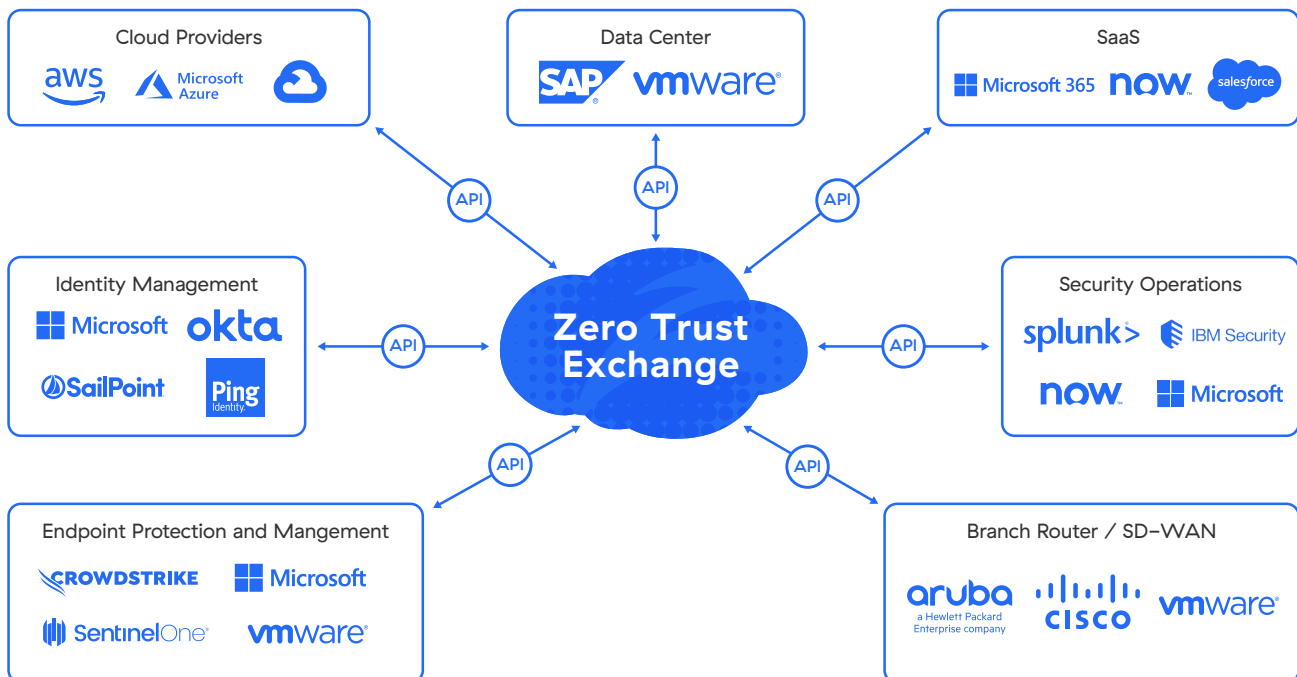


Figure 2: Zscaler Internet Access partner ecosystem

**TABLE 1: ZSCALER INTERNET ACCESS FEATURES AND CAPABILITIES**

FEATURE	DETAILS
<b>Capabilities</b>	
URL filtering	Allow, block, caution, or isolate user access to specified web categories or destinations to stop web-based threats and ensure compliance with organizational policies.
SSL inspection	Get unlimited TLS/SSL traffic inspection to identify threats and data loss hiding in encrypted traffic. Specify which web categories or apps to inspect based on privacy or regulatory requirements.
DNS security	Identify and route suspicious command-and-control connections to Zscaler threat detection engines for full content inspection.
File control	Block or allow file download/upload to applications based on app, user, or user group.
Bandwidth control	Enforce bandwidth policies and prioritize business-critical applications over recreational traffic.
Advanced threat protection	Stop advanced cyberattacks like malware, ransomware, supply chain attacks, phishing, and more with proprietary advanced threat protection. Set granular policies based on your organization's risk tolerance.
Inline data protection (data in motion)	Use forward proxy and SSL inspection capabilities to control the flow of sensitive information to risky web destinations and cloud apps in real time, stopping internal and external threats to data. Advanced inline protection is provided whether an app is sanctioned or unmanaged without requiring network device logs.
Out-of-band data protection (data at rest)	Use API integrations to scan SaaS apps, cloud platforms, and their contents to identify sensitive data at rest and remediate automatically by revoking risky or external shares, for example.
Intrusion prevention	Get complete threat protection from botnets, advanced threats, and zero-days, along with contextual information about the user, app, and threat. Cloud IPS works seamlessly across Cloud Firewall, Cloud Sandbox, Cloud DLP, and CASB.
Dynamic, risk-based access and security policy	Automatically adapt security and access policy to user, device, application, and content risk.
Malware analysis	Detect, prevent, and quarantine unknown threats hiding in malicious payloads inline with advanced AI/ML to stop patient-zero attacks.
DNS filtering	Control and block DNS requests against known and malicious destinations.
Web isolation	Make web-based threats obsolete by delivering active content as a benign stream of pixels to the end user's browser.
Correlated threat insights	Speed investigation and response times with contextualized and correlated alerts with insights into threat score, affected asset, severity, and more.
Application isolation	Allow safe, agentless unmanaged device access to SaaS, cloud, and private apps with granular control over user actions like copy/paste, upload/download, and print to stop sensitive data loss.
Digital experience monitoring	Get a unified view of application, cloud path, and endpoint performance metrics for analysis and troubleshooting.
Application isolation	Allow safe, agentless unmanaged device access to SaaS, cloud, and private apps with granular control over user actions like copy/paste, upload/download, and print to stop sensitive data loss.
Workload-to-internet communication protection	Prevent compromise and stop lateral movement for workload-to-internet communications. Includes SSL inspection, IPS, URL filtering, and data protection for all communication.

FEATURE	DETAILS
Platform features	
Flexible connectivity options	<ul style="list-style-type: none"> <li>• <b>Zscaler Client Connector (ZCC):</b> Forward traffic to the Zero Trust Exchange via a lightweight agent that supports Windows, macOS, iOS, iPadOS, Android, and Linux.</li> <li>• <b>GRE or IPsec tunnels:</b> Use GRE and/or IPsec tunnels to send traffic to the Zero Trust Exchange for devices without ZCC.</li> <li>• <b>Browser isolation:</b> Seamlessly connect any BYOD or unmanaged devices with integrated Cloud Browser Isolation.</li> <li>• <b>Proxy chaining:</b> Zscaler supports forwarding traffic from one proxy server to another, but this is not recommended in production environments.</li> <li>• <b>PAC files:</b> Send traffic to the Zero Trust Exchange with PAC files for devices without ZCC.</li> </ul>
Cloud-delivered deployment	100% cloud-native platform delivered as a SaaS service. For unique use cases, private and virtual service edges are available.
Data privacy and retention	<p>When logging data, content is never written to the disk and there are granular controls to determine where exactly logging takes place. Use role-based access control (RBAC) to provide read-only access, username anonymization/obfuscation, and separate access rights by department or function, in accordance with key compliance regulations.</p> <p>Data is retained for a rolling period of six months or less, depending on the product. You can purchase additional storage that retains data for as long as desired.</p>
Key compliance certifications	<p>Certifications include:</p> <ul style="list-style-type: none"> <li>• FedRAMP</li> <li>• ISO 27001</li> <li>• SOC 2 Type II</li> <li>• SOC 3</li> <li>• NIST 800-63C</li> </ul> <p>See the full list of our compliance certifications <a href="#">here</a>.</p>
Granular API support	<p>We maintain REST API integrations with numerous identity, networking, and security vendors. For example, you can share logs between Zscaler and your cloud-based or on-prem SIEM (e.g., Splunk).</p> <p><a href="#">Learn more</a></p>
Direct peering	Direct peering with major internet and SaaS providers and public cloud destinations ensures the fastest traffic path possible.
Service level agreements (SLAs)	
Availability	99.999%, measured by transactions lost
Proxy latency	< 100 ms, including when threat and DLP scanning is on
Virus capture	100% of known viruses and malware
Supported platforms & systems	
Client Connector	<p>Support for:</p> <ul style="list-style-type: none"> <li>• iOS 9 or later</li> <li>• Android 5 or later</li> <li>• Windows 7 and later</li> <li>• Mac OS X 10.10 and later</li> <li>• CentOS 8</li> <li>• Ubuntu 20.04</li> </ul> <p><a href="#">Learn more</a></p>



## ZIA editions

ZIA EDITIONS OVERVIEW	BUSINESS	TRANSFORMATION	UNLIMITED
Secure web gateway	✓	✓	✓
Full TLS/SSL inspection	✓	✓	✓
URL filtering	✓	✓	✓
Cloud application visibility and control	✓	✓	✓
Inline malware prevention	✓	✓	✓
AI-powered phishing and C2 detection	✓	✓	✓
Data protection essentials (DLP, visibility, and alerting; CASB, 1 app)	✓	✓	✓
Standard digital experience monitoring	✓	✓	✓
Cloud-gen firewall and IPS	Add-on	✓	✓
Cloud-gen sandbox with AI-powered quarantine	Add-on	✓	✓
Attacker deception	Add-on	✓	✓
Dynamic, risk-based policy	-	✓	✓
Contextual alerts	-	✓	✓
AI-powered Cloud Browser Isolation	Add-on	✓	✓
Data Protection Advanced Plus (Inline web, SaaS, email, advanced classification, incident management)	Add-on	Add-on	✓
IoT, server, and guest Wi-Fi protection	Add-on	Add-on	✓

### Licensing model

All Zscaler Internet Access editions are priced per user. For certain products inside of your edition, pricing may vary outside of user count. For more information on pricing, talk to your Zscaler account team.

## Part of the holistic Zero Trust Exchange

The Zero Trust Exchange enables fast, secure connections and allows your employees to work from anywhere using the internet as the corporate network. Based on the zero trust principle of least-privileged access, it provides comprehensive security using context-based identity and policy enforcement.



#### About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at [zscaler.com](https://zscaler.com) or follow us on Twitter @zscaler.

© 2022 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at [zscaler.com/legal/trademarks](https://zscaler.com/legal/trademarks) are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.